UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Room 409 of the Extended Stay America at 4020 Hauck Road, Cincinnati, OH 45241

Case No. **1:23-MJ-00940**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-3 (incorporated by reference).

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 922(a)(6), 371	False Statement During Purchase of a Firearm, Conspiracy

The application is based on these facts:

See Attached Affidavit (incorporated by reference).

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Derek Graham
Applicant's signature

Derek Graham, Special Agent, ATF
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime Video Conference *(specify reliable electronic means)*.

Date: **Nov 15, 2023**

Stephanie K. Bowman
Judge's signature

City and state: Cincinnati, Ohio

Hon. Stephanie K. Bowman, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A-3

Property to be Searched

The property to be searched, **SUBJECT PREMISES – EXTENDED STAY**, is Room 409 of the Extended Stay America hotel located at 4020 Hauck Road, Cincinnati, OH 45241. The entrance to the hotel is pictured below. Room 409 is on the fourth floor. The door to Room 409 is marked with a dark-gray rectangle reading "409." The door appears to be made of brown wood or have a wood façade, and it has a silver door with a space for a keycard.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 922(a)(6) (False Statement During Purchase of a Firearm) and 371 (Conspiracy) involving TIMOTHY MOORMAN and other known and unknown coconspirators and occurring after on or about September 1, 2023, including:

   a. Records and information relating to the purchase, attempted purchase, acquisition, possession, sale, and/or transfer of firearms, ammunition, and/or firearms accessories;

   b. Records and information relating to the making of false statements during the purchase of a firearm;

   c. Records and information relating to the identity of coconspirators to the Target Offenses;

   d. Records and information relating to preparatory steps taken in furtherance of the Target Offenses;

   e. Records and information relating to steps taken to evade capture for the Target Offenses;

   f. Records and information relating to communications between any coconspirators involved in the Target Offenses;

   g. Records and information relating to the proceeds of the Target Offenses, including but not limited to information about financial accounts used to receive, possess, store, and transfer criminal proceeds;

h. Records and information relating to occupancy at, and/or control over, a premises or vehicle, including but not limited to rental agreements and records, leases, mail, vehicle registrations, utility bills and receipts, and personal identification and photographs.

2. Firearms, ammunition, holsters, gun cases, gun boxes, and other firearms accessories.

3. Copies of ATF Forms 4473s, and any related purchase and sale documents and receipts.

4. Any U.S. currency in an amount of at least $100 that constitutes evidence of, or the proceeds of, firearm sales.

5. Keys, key fobs, garage door openers, and other items that can be used to access a vehicle or premises.

6. Financial instruments used in furtherance of violations of the Target Offenses, or that constitute proceeds of violations of the Target Offenses, including but not limited to credit cards, debit cards, prepaid cards, money orders, and cashier's checks.

7. Computers or storage media used as a means to commit the violations described above.

8. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

i. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and

passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

v. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

vi. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

viii. evidence of the times the COMPUTER was used;

ix. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

x. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

xi. records of or information about Internet Protocol addresses used by the COMPUTER;

xii. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

xiii. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the Premises described in Attachments A-1 through A-4, law enforcement personnel are authorized to (1) press or swipe the fingers (including

thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF THE FOUR LOCATIONS DESCRIBED IN ATTACHMENTS A-1 THROUGH A-4	Case No. **1:23-MJ-00940** **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Derek Graham, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications under Federal Rule of Criminal Procedure 41 for warrants to search the premises listed below, further described in Attachments A-1 through A-4, for the things described in Attachment B:

- **The person of TIMOTHY MOORMAN, DOB 12/XX/1991, SSN XXX-XX-9042**
- [redacted] **Road, Cincinnati, OH 45251 ("SUBJECT PREMISES – WUEST ROAD")**
- **Room 409 of the Extended Stay America at 4020 Hauck Road, Cincinnati, OH ("SUBJECT PREMISES – EXTENDED STAY")**
- **The white 2022 Jeep Compass bearing Ohio Registration** [redacted] **and VIN 3C4NJDBB7NT215734 (the "COMPASS")**

(collectively, the **"SUBJECT PREMISES"**).

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF), and have been so employed since October of 2007. As a part of my training with the ATF, I graduated from the Federal Law Enforcement Training Center, Criminal Investigator School, located in Brunswick, Georgia. I graduated from the ATF Special Agent Basic Training Academy, located in Brunswick, Georgia, in April 2008. Prior to my employment with ATF, I was a Federal Air Marshal in the Department of Homeland Security from June 2006 through

October 2007. In addition, I was a Criminal Research Specialist with the Washington, DC High Intensity Drug Trafficking Area/Drug Enforcement Administration from June 2003 through June 2006. I am a graduate of Augustana College, where I received a Bachelor's degree in Business Administration in May of 2002. I am also a graduate of Boston University, where I received a Master's degree in Criminal Justice in June of 2006.

3. I have experience in the investigation, apprehension, and prosecution of individuals suspected of being involved in federal firearms and drug offenses. I have specific experience in investigating the use of cell phones by criminal suspects who are involved in the commission of those offenses. I have been trained by ATF as a Digital Media Collection Specialist (DMCS) and have completed more than 285 forensic extractions of cellular telephones, computers, and other electronic storage media. I have also reviewed forensic extractions of cellular telephones, computers, and other electronic storage media, and have examined content and communications contained within these devices obtained by forensic extraction. This content includes records of communication through call logs, text message content, images and videos, and communication made through various social media applications.

4. I know from training and experience that individuals typically keep cell phones in their residences, on their persons, or within their immediate control, such as in the cupholder of a car they are driving, because cell phones are regularly used and possessed as an item of personal property. I also know from my training and experience that in today's age it is typical for individuals engaged in criminal activity to possess multiple active cellular phones at one time. For example, many criminals have one phone that they use for personal communications (e.g., with family members) and another phone that they use to communicate with criminal associates.

5. I also know based on my training and experience that, when individuals are involved in an illegal business, such as firearms or drug trafficking, those individuals commonly maintain in their residences and stash houses,[1] on their persons, and/or in their vehicles lists of customers, supplier lists, pay/owe sheets, receipts, address books, and other documents listing the price and quantity of items sold, as well as the date the items were purchased, possessed, and sold. These records may be stored in paper form or on electronic devices, such as cell phones and other electronic storage media.

6. Additionally, based on my training and experience, I know that firearms traffickers commonly store in their residences, stash houses, and/or vehicles, as well as carry on their persons, fruits and contraband of their trafficking, such as firearms, ammunition, firearms accessories, and the proceeds of their trafficking. It is also common for individuals to carry on their person or in their vehicles, or to store in premises they control, items allowing them to access those premises, such as house keys and garage-door openers, as well as documentation showing their association with certain premises, such as identification cards and other paperwork listing home addresses.

7. Through training and experience, I have become familiar with firearms trafficking investigations and the analysis of ATF Form 4473s, ATF Trace Reports[2], ATF Multiple Sales

---

[1] Based on my training and experience, I know that the term "stash house" refers to a location where a suspect typically does not reside but instead uses for purposes of criminal activity. For example, drug traffickers commonly store drugs and drug proceeds in stash houses. In my experience, criminals commonly use stash houses in an attempt to distance themselves from the evidence of their criminal activity.

[2] An ATF Trace Report is a document detailing the information about the purchase of a firearm and the information related to the recovery of the firearm. The information contained in the ATF Trace Report is obtained upon request by a law enforcement agency to identify the original purchaser of a recovered firearm. A completed ATF Trace Report includes the identifying information of the firearm, including the recovery location and date; the Federal Firearms Licensee that transferred the firearm; and the information related to the purchaser of the firearm, which is obtained

Reports[3], and Federal Firearms Licensees Acquisition and Disposition Records[4]. I'm also experienced in analyzing ATF Trace Reports and ATF Multiple Sales Reports and identifying patterns and purchasing activity of suspected firearms traffickers. This includes the analysis of the number of days between the purchase of a firearm and the subsequent date law enforcement authorities recover said firearm(s). Analysis additionally involves the examination of relevant ATF Trace Reports and ATF Multiple Sales Reports involving a specific purchaser or possessor, and/or the volume or make and model of particular firearms identified as being purchased by suspects of firearms trafficking.

8. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrants and does not set forth all my knowledge about this matter.

9. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 922(a)(6) (False Statement During Purchase of a Firearm) and 371 (Conspiracy) have been committed by TIMOTHY MOORMAN and other known and unknown coconspirators. There is also probable cause to search the locations described in Attachments A-1

---

from the ATF Form 4473 – Firearms Transaction Record, provided by the Federal Firearms Licensee to the ATF National Tracing Center at the time firearm trace is requested.

[3] An ATF Multiple Sale Report documents the information about the purchase of two or more pistols or revolvers by an individual at one time, or during five consecutive business days, from the same Federal Firearms Licensee. The Federal Firearms Licensee is required to complete an ATF Form 3310.4 – Report of Multiple Sale or Other Disposition of Pistols and Revolvers and submit this form to ATF.

[4] Acquisition and Disposition Records are required to be maintained by Federal Firearms Licensees, which documents all firearms that a Federal Firearms Licensee receives into, and distributes from, their inventory.

through A-4 for the evidence, instrumentalities, fruits, and contraband of these crimes further described in Attachment B.

PROBABLE CAUSE

A. Introduction

9. The United States is conducting an investigation of TIMOTHY MOORMAN and several other suspects regarding possible violations of 18 U.S.C. §§ 922(a)(6) and 371.

10. [redacted] law enforcement personnel recovered the abandoned backpack, which contained thirty-six firearms.

11. The firearms were submitted for tracing, which revealed that eight of them had been purchased by TIMOTHY MOORMAN just days before, from October 16, 2023, through October 21, 2023. All of the purchases were from Federal Firearms Licensees (FFLs) in Cincinnati. Further investigation revealed that MOORMAN had bought a total of twenty-two firearms, all handguns, from Cincinnati FFLs from September 29 through October 27, 2023.

12. I am now seeking warrants for MOORMAN's person, his vehicle, his home, and the hotel he has been renting for several weeks, because, as I explain in this affidavit, there is probable cause to believe that these locations will contain evidence, instrumentalities, fruits, and contraband of violations of 18 U.S.C. §§ 922(a)(6) and 371.

B. On October 26, 2023, [redacted] law enforcement [redacted] recovered thirty-six firearms from an abandoned bag after a suspected smuggling attempt.

13. [redacted]

16. [redacted] law enforcement recovered the abandoned backpack, which contained thirty-six handguns.

---

[5] [redacted].

[redacted]

C. Eight of the thirty-six firearms recovered on October 26, 2023, had been purchased by MOORMAN in Cincinnati.

20. The firearms recovered by [redacted] law enforcement on October 26, 2023, were submitted for tracing, which revealed that eight of the thirty-six firearms had been purchased by MOORMAN at FFLs in Cincinnati, Ohio, from October 16 through 21, 2023. Specifically:

A. MOORMAN purchased a Glock 43x bearing Serial No. AHVB218 from Bass Pro Shops Store #011 on October 21, 2023.

B. MOORMAN purchased a Springfield Armory Hellcat bearing Serial No. BE100458, a Glock 43x bearing Serial No. CBGV468, and a Glock 43x bearing Serial No. CAZG326 from Range USA – Cincy West on October 19, 2023.

C. MOORMAN purchased a Glock 23 Gen 5 bearing Serial No. CAKR580 and a Glock 43 bearing Serial No. AHZD477 from Range USA – Cincy West on October 16, 2023.

D. MOORMAN purchased a Glock 43x bearing Serial No. BZVM543 and a Glock 43x bearing Serial No. CACT219 from Bass Prop Shops Store #011 on October 16, 2023.

21. I have reviewed ATF Form 4473s and Multiple Sales Reports and learned that from September 29, 2023, through October 27, 2023, MOORMAN purchased a total of twenty-two firearms from FFLs in Cincinnati, OH. The firearms purchased by MOORMAN at each FFL are detailed in the table below, with the recovered firearms[6] in bold type:

[6] The recovered firearms in bold are the same firearms described above that were recovered near [redacted]

FFL	Date	F/A Make	F/A Model	F/A Serial No.
North College Hill Gun Store	10/27/2023	Glock	23	CBGF444
North College Hill Gun Store	10/27/2023	Glock	27	BY2K652
North College Hill Gun Store	10/27/2023	Glock	19	CBNR555
Target World	10/27/2023	Glock	TBD	TBD
Range USA - Blue Ash	10/26/2023	Glock	19 Gen 5	BWYT942
Range USA - Blue Ash	10/26/2023	Glock	43x	CAUM316
Range USA - Blue Ash	10/25/2023	Glock	26	AGKD179
Range USA - Blue Ash	10/25/2023	Glock	27 Gen 5	BYGL310
Range USA - Cincy West	10/24/2023	Glock	28 Gen 3	AHSP847
Range USA - Cincy West	10/24/2023	Glock	28 Gen 3	AHSF892
Range USA - Cincy West	10/24/2023	Glock	26	CAKU238
Range USA - Cincy West	10/24/2023	Canik Century Arms	TP9 Elite SC	23CB07572
Bass Pro Shops	**10/21/2023**	**Glock**	**43x**	**AHVB218**
Bass Pro Shops	10/21/2023	Glock	30	CAZA625
Range USA - Cincy West	**10/19/2023**	**Glock**	**43x**	**CBGV468**
Range USA - Cincy West	**10/19/2023**	**Glock**	**43x**	**CAZG326**
Range USA - Cincy West	**10/19/2023**	**Springfield Armory**	**Hellcat**	**BE100458**
Range USA - Cincy West	**10/16/2023**	**Glock**	**23 Gen 5**	**CAKR580**
Range USA - Cincy West	**10/16/2023**	**Glock**	**43**	**AHZD477**
Bass Pro Shops	**10/16/2023**	**Glock**	**43x**	**BZVM543**
Bass Pro Shops	**10/16/2023**	**Glock**	**43x**	**CACT219**
Bass Pro Shops	9/29/2023	Glock	23	BZNF591

22. The approximate price for the twenty-two firearms purchased from September 29, 2023, through October 27, 2023, was $11,565.[7]

23. Based on my experience with firearms trafficking investigations, and indicators of suspected firearms trafficking—including the facts described above suggesting that the firearms [redacted] I believe the short time period from when the firearms were purchased by MOORMAN to when they were recovered by [redacted] law enforcement is an indicator that these

[7] The actual price of some of the firearms purchased from North College Hill Gun Store and Bass Pro Shops was not available at the time this affidavit was written. For those firearms, I used the known price paid for the same make and model firearms from other FFLs to estimate the purchase price.

firearms were not purchased for personal possession, but were in fact straw purchases (meaning that MOORMAN bought them for someone else).

24. I also noted that all of the firearms recovered in [redacted] were ones MOORMAN had purchased from October 16, 2023, through October 21, 2023. He bought twelve additional firearms after that date, suggesting that, if he has not yet handed the firearms off to a coconspirator to [redacted] they are likely still in his possession.

D. During the firearms purchases, MOORMAN listed SUBJECT PREMISES – WUEST ROAD, which is also on his driver's license, as his current residence.

25. On each ATF Form 4473 for the purchases listed above, MOORMAN documented his residence as [redacted] Road, Cincinnati, OH (the **SUBJECT PREMISES – WUEST ROAD)**.

26. On November 8, 2023, I queried a database available to law enforcement that includes State-issued identification information about Ohio residents. I determined that MOORMAN has a current Ohio Driver's License issued to him documenting his address as the **SUBJECT PREMISES – WUEST ROAD.**

E. MOORMAN appears to live at the SUBJECT PREMISES – WUEST ROAD with his parents, and a white Jeep Compass he uses is also registered at that address.

27. On November 8, 2023, I queried the address of "[redacted] Road" in the Hamilton County Auditor records and learned that the **SUBJECT PREMISES – WUEST ROAD** is currently owned by [redacted] and [redacted]

28. On November 8, 2023, I queried a database containing Ohio State Identification information and determined that [redacted] (DOB 03/XX/1964) and [redacted] (DOB 01/XX/1968) both have current Ohio State Identification cards listing the address of **SUBJECT PREMISES – WUEST ROAD.** In addition, based on MOORMAN's birth year being 1991, and

information later provided by Individual 1, described below, [redacted]

29. On November 9, 2023, ATF Task Force Officer (TFO) Joseph Ruchti queried the same database containing Ohio State Identification information for vehicles registered to the **SUBJECT PREMISES – WUEST ROAD.** TFO Ruchti identified a white 2022 Jeep Compass, with Ohio Registration [redacted] and VIN 3C4NJDBB7NT215734 (the "**COMPASS")**, registered to "Moorman Insurance, Inc." at **SUBJECT PREMISES – WUEST ROAD.** I believe based on evidence I describe below, including surveillance video from area FFLs, physical surveillance from November 14, 2023, and [redacted] that MOORMAN operates and has control over the **COMPASS.**

F. A recent domestic violence charge against MOORMAN provided additional evidence that MOORMAN lives at SUBJECT PREMISES – WUEST ROAD.

30. On October 30, 2023, Cincinnati Police Department (CPD) Police Officer Jesse Hooven obtained an arrest warrant for MOORMAN from the Hamilton County Municipal Court in relation to an alleged Domestic Violence incident by MOORMAN against the victim, Individual 1. The incident was alleged to have occurred on October 30, 2023.

31. [redacted]

32. [redacted]

[redacted]

36. A review of the Form 4473s for MOORMAN's purchases shows that he listed phone number [redacted]3019 on the forms he submitted at Range USA – Cincy West and Range USA – Blue Ash on October 24, 25, and 26, 2023. On the Form 4473s submitted at Range USA – Cincy West on October 16 and 19, 2023, and at Target World on October 26, 2023, he listed phone number [redacted] 6252.

37. On November 8, 2023, I queried a database available to law enforcement for the above-described telephone numbers and found that both were associated with MOORMAN.

38. Based on provided by AT&T on November 9, 2023, and a discussion with a representative from AT&T, I learned that the account for telephone number [redacted]6252 was

cancelled on October 7, 2023, and that it had been subscribed in the name of "Timothy Moorman" at the address of the **SUBJECT PREMISES – WUEST ROAD**.

39. Although, as I describe below, MOORMAN has had a reservation at an Extended Stay hotel (**SUBJECT PREMISES – EXTENDED STAY)** for a little more than a month, I respectfully submit that there is probable cause to believe that MOORMAN is still living at, and still has control over, **SUBJECT PREMISES – WUEST ROAD—**and therefore that it will contain evidence of the crimes under investigation. First, property records show that **SUBJECT PREMISES – WUEST ROAD** has been [redacted] (i.e., since 1993, when he was approximately two years old). [redacted] shows that Individual 1 and MOORMAN were living at **SUBJECT PREMISES – WUEST ROAD** at least as of October 2023, when the incident of domestic violence is alleged to have occurred—suggesting that MOORMAN has continued to have a room in the home even in his adulthood, especially given that he appears to be unemployed. As I describe below, MOORMAN began renting a room at the Extended Stay on October 9, 2023—several weeks before the alleged incident of domestic violence—suggesting, based on my training and experience, that he was using it as a stash house even while living at **SUBJECT PREMISES – WUEST ROAD**. Given MOORMAN's longtime, and recent, association with **SUBJECT PREMISES – WUEST ROAD**, and because it is unlikely (simply from a practical perspective) that MOORMAN moved all of his belongings into a hotel room, there is reason to believe that he still has a room at **SUBJECT PREMISES – WUEST ROAD** and keeps at least some of his belongings there. I further submit that, for all the reasons given in this affidavit about why evidence, instrumentalities, fruits, and contraband of the Target Offenses are likely to be found in a suspect's residence, **SUBJECT PREMISES – WUEST ROAD** likely contains the items described in Attachment B.

G. Surveillance video from Range USA and recent physical surveillance show TIMOTHY MOORMAN operating the COMPASS.

40. Surveillance video from Range USA related to the firearm purchases by MOORMAN shows him arrive and depart Range USA driving a white newer-model Jeep Compass. Based on the registration information I described above and the surveillance I describe below, I believe this vehicle was the **COMPASS.** MOORMAN is also on video operating a vehicle consistent in appearance with the **COMPASS** before and after the purchases from two Range USA locations on October 16, 19, and 24 through 26, 2023.

41. On November 14, 2023, ATF agents and CPD officers conducted surveillance of MOORMAN and saw him get into and out of the **COMPASS** on several occasions over several hours.

42. Based on the fact that MOORMAN used a white Jeep Compass during the firearms purchases at Range USA, the fact that [redacted] the fact that a white 2022 Jeep Compass is registered to a business at the **SUBJECT PREMISES – WUEST ROAD**, and the surveillance from November 14, 2023, putting MOORMAN in the **COMPASS**, I believe MOORMAN has control of and uses the **COMPASS.** I further submit that, for the reasons given above about th[redacted] items likely to be in a suspect's vehicle, there is probable cause to believe that the **COMPASS** will contain the items listed in Attachment B.

H. MOORMAN has had a reservation at SUBJECT PREMISES – EXTENDED STAY since October 9, 2023, and was seen there on November 14, 2023.

43. On November 14, 2023, agents and officers conducted surveillance of MOORMAN and saw him come out of the Extended Stay at 4020 Hauck Road, Cincinnati, OH 45241 (i.e., the

SUBJECT PREMISES – EXTENDED STAY). MOORMAN got into the **COMPASS** as the driver and drove away.

44. That same day, a representative of the Extended Stay provided a copy of their guest list, which showed that MOORMAN had begun renting a room on October 9, 2023, and had a checkout date of November 30, 2023. The records showed that he was staying in room 409 **(i.e., SUBJECT PREMISES – EXTENDED STAY).**

45. Based on my training and experience, a hotel room being used by a suspect for an extended period is likely to contain evidence, instrumentalities, fruits, and contraband of the Target Offenses for all the same reasons a suspect's primary residence is. In this case, I respectfully submit that there is additional reason to believe that MOORMAN is storing contraband, including firearms, at the **SUBJECT PREMISES – EXTENDED STAY** because, based on my training and experience, suspects commonly seek to hide evidence of their criminal activities by using stash houses and other locations that are not easily linked to them. In this case, for example, law enforcement was only able to find the **SUBJECT PREMISES – EXTENDED STAY** by checking license plate readers for hits on the **COMPASS**; MOORMAN's name did not show up in law enforcement databases as associated with this hotel. Additionally, because **SUBJECT PREMISES – WEUST ROAD** is a residence MOORMAN shares with his parents, it is likely that he is using **SUBJECT PREMISES – EXTENDED STAY** as a stash house in an attempt to hide his criminal activities from his parents.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

46. As described above and in Attachment B, this application seeks permission to search for records that might be found on each of the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or

other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

47. *Probable cause.* I submit that if a computer or storage medium is found on any of the **SUBJECT PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

A. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

B. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

C. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system

data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

D. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

48. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

B. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the

suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

C. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the

computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

E. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

49. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

A. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine

storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

B. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

C. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

50. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

51. Because several people may share some of the **SUBJECT PREMISES** as a residence, and/or because more than one person may use some of the vehicles at issue, it is possible that the **SUBJECT PREMISES** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

USE OF BIOMETRIC FEATURES

52. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to use.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home"

button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that

biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the **SUBJECT PREMISES** and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement

personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

REQUEST FOR SEALING

53. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Derek Graham

DEREK GRAHAM
Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed and sworn to before me by reliable electronic means, specifically, FaceTime video conference on November 15, 2023.

Stephanie K. Bowman

HON. STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-3

Property to be Searched

The property to be searched, **SUBJECT PREMISES – EXTENDED STAY**, is Room 409 of the Extended Stay America hotel located at 4020 Hauck Road, Cincinnati, OH 45241. The entrance to the hotel is pictured below. Room 409 is on the fourth floor. The door to Room 409 is marked with a dark-gray rectangle reading "409." The door appears to be made of brown wood or have a wood façade, and it has a silver door with a space for a keycard.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 922(a)(6) (False Statement During Purchase of a Firearm) and 371 (Conspiracy) involving TIMOTHY MOORMAN and other known and unknown coconspirators and occurring after on or about September 1, 2023, including:

   a. Records and information relating to the purchase, attempted purchase, acquisition, possession, sale, and/or transfer of firearms, ammunition, and/or firearms accessories;

   b. Records and information relating to the making of false statements during the purchase of a firearm;

   c. Records and information relating to the identity of coconspirators to the Target Offenses;

   d. Records and information relating to preparatory steps taken in furtherance of the Target Offenses;

   e. Records and information relating to steps taken to evade capture for the Target Offenses;

   f. Records and information relating to communications between any coconspirators involved in the Target Offenses;

   g. Records and information relating to the proceeds of the Target Offenses, including but not limited to information about financial accounts used to receive, possess, store, and transfer criminal proceeds;

h. Records and information relating to occupancy at, and/or control over, a premises or vehicle, including but not limited to rental agreements and records, leases, mail, vehicle registrations, utility bills and receipts, and personal identification and photographs.

2. Firearms, ammunition, holsters, gun cases, gun boxes, and other firearms accessories.

3. Copies of ATF Forms 4473s, and any related purchase and sale documents and receipts.

4. Any U.S. currency in an amount of at least $100 that constitutes evidence of, or the proceeds of, firearm sales.

5. Keys, key fobs, garage door openers, and other items that can be used to access a vehicle or premises.

6. Financial instruments used in furtherance of violations of the Target Offenses, or that constitute proceeds of violations of the Target Offenses, including but not limited to credit cards, debit cards, prepaid cards, money orders, and cashier's checks.

7. Computers or storage media used as a means to commit the violations described above.

8. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

i. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and

passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

v. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

vi. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

viii. evidence of the times the COMPUTER was used;

ix. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

x. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

xi. records of or information about Internet Protocol addresses used by the COMPUTER;

xii. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

xiii. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the Premises described in Attachments A-1 through A-4, law enforcement personnel are authorized to (1) press or swipe the fingers (including

thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.